BOTNETS, ZOMBIES, AND IRC SECURITY

Investigating Botnets, Zombies, and IRC Security

Seth Thigpen

East Carolina University

Abstract

The Internet has many aspects that make it ideal for communication and commerce. It makes selling products and services possible without the need for the consumer to set foot outside his door. It allows people from opposite ends of the earth to collaborate on research, product development, and casual conversation.

Internet relay chat (IRC) has made it possible for ordinary people to meet and exchange ideas. It also, however, continues to aid in the spread of malicious activity through botnets, zombies, and Trojans. Hackers have used IRC to engage in identity theft, sending spam, and controlling compromised computers. Through the use of carefully engineered scripts and programs, hackers can use IRC as a centralized location to launch DDoS attacks and infect computers with robots to effectively take advantage of unsuspecting targets.

Hackers are using zombie armies for their personal gain. One can even purchase these armies via the Internet black market. Thwarting these attacks and promoting security awareness begins with understanding exactly what botnets and zombies are and how to tighten security in IRC clients.

Investigating Botnets, Zombies, and IRC Security

Introduction

The Internet has become a vast, complex conduit of information exchange. Many different tools exist that enable Internet users to communicate effectively and efficiently. Some of these tools have been developed in such a way that allows hackers with malicious intent to take advantage of other Internet users.

Hackers have continued to create tools to aid them in their endeavors. The use of robots (usually referred to as bots) has proved to be an effective method for these hackers to infiltrate remote systems. Installing bots on Internet users' computers allows the hacker to carry out attacks on a large scale. These attacks can be extremely harmful to businesses and individuals alike. Identity theft, denial of service, and spam are a few of the threats in which a hacker may use a bot as the primary tool.

IRC

IRC is an acronym that stands for Internet Relay Chat. Originally developed by Jarkko Oikarinen, the purpose of this software is to allow computer users to chat in real time. (Oikarinen) The client-server software has been steadily developed and improved upon over the years. IRC has expanded into multiple networks which include hundreds of servers.

The core of the IRC network is the server. The server supplies the necessary components in order to allow clients to connect and communicate. Communication through IRC is not direct peer to peer. Instead, all packets are relayed through the server to reach the destination. Hence relay in the name of the protocol. There are numerous IRC server daemons available for

different operating systems which include: Bahamut, Undernet IRCD, UnrealIRCd, IRCD, Global IRC-d, and DICE. This is not an exhaustive list by far.

Many different client programs are available to work with these servers. This client software allows the user to join channels and interact with other users. Some of the most popular IRC clients are: mIRC, XChat, ircII, Bersirc, and bitchx. IRC clients can even be embedded in HTML (possibly via Java) to allow website visitors to chat with other visitors currently viewing the website.

IRC servers create channels to allow users to communicate with a subset of server users. A user can define in a command the channel he wishes to join. When the first user attempts to join a channel, the channel is formed. When the last user parts the channel, the channel is removed. (Oikarinen and Reed, 1993) That is, unless the network employs the help of a bot dedicated to maintaining channels.

Many IRC servers also include service users. These service users are essentially robots which provide services to users. These service bots are usually named in a fashion that makes them easy to recognize such as Chanserv, Nickserv, Memoserv, etc. One common service is that of a Channel bot. Chanserv (most commonly used name) can help maintain channels even while no users are currently in that channel. Each implementation of a channel bot differs; therefore, features present on the bot may differ from network to network.

Since information is relayed in IRC, this type of communication is not secure. There are many possible ways for attackers to probe for information and initiate attacks. Trojans, viruses, and backdoors are some of the malicious tools that hackers on IRC use to compromise computers.

Most IRC clients allow scripting to make usage easier and automate repetitive tasks. A simple script could be used to authenticate a user to the service monitoring nick names. Scripting in IRC clients allows the use of many techniques found in popular programming languages but these scripts are not as robust as the languages themselves. Variables, switch statements, if-then, comparisons, timers, and many other functions are available to provide the tools necessary to create useful scripts. The following is a small snippet of code from a script written to monitor an automated advertisement to a channel.

Sample IRC Script

```
/checkchan {
  if ($me ison %adchan && %adcount < 3) {
    msg %adchan %temp
    inc %adcount
    echo ----------------------
    echo Advertisement #: %adcount
    echo ----------------------
    if ($me ison %homechan) {
      msg %homechan %temp
    }
  }
  else {
    echo •4 ********************************************************************
    echo •4 35 seconds have not passed yet, Ignoring Command (Ban Protection)
    echo •4 ********************************************************************
  }
}
```

The previous script is extremely simple. Advanced programmers can write code that does exhaustive, time consuming scans and data collection. This is one of the issues surrounding the security of IRC. Other network users cannot be trusted on these networks.

Zombies

The term zombie most often represents the living dead. The Merriam-Webster Online Dictionary (2005) defines a zombie as "a will-less and speechless human … capable only of automatic movement who is held to have died and been supernaturally reanimated." A computer zombie shares attributes with this definition. Webopedia defines a zombie as: "A computer that has been implanted with a daemon that puts it under the control of a malicious hacker without the knowledge of the computer owner." (2005) This second definition is most applicable to this

discussion. Computer zombies are lifeless soldiers controlled by an attacker who follow instructions without complaint.

Hackers need multiple computers to carry out many attacks. A collection of zombie computers is referred to as a botnet. "Botnet is a jargon term for a collection of software robots, or bots, which run autonomously. A botnet's originator can control the group remotely, usually through a means such as IRC, and usually for nefarious purposes." (Botnet, 2005) This zombie army can represent a dangerous threat to large and small companies alike on the Internet.

The process of creating a zombie may vary, but the basic idea is as follows. A hacker finds a target computer and gains access. The attacker may gain access by guessing a username and password combination, buffer overflow attack, backdoor, or other known exploit. After the attacker gains control of the machine, he loads a program that will enable the computer to execute commands given to it via an IRC channel. The newly created zombie joins the predetermined channel and waits for further instruction.

Bots used to control a zombie usually have tools installed that can aid in many different functions. Some of these bots initiate DoS attacks via ICMP, TCP, and UDP; rummage through the Windows registry to collect software keys; make changes to the registry; conduct bandwidth tests; and even act as an IRC daemon to allow other bots to connect and expand the botnet. (Schluting, 2005) In the case of a distributed denial of service (DDoS), the attacker waits until he has enough zombies under his control and idling in the IRC channel. He can then issue a series of commands to carry out the attack. Each zombie mindlessly executes the commands it has been given.

Botnets Usage

Botnets are almost always created to conduct malicious activity. However, there are a few distributed computing projects currently in progress that could be viewed as botnets. SETI@Home and Folding@Home are two examples of distributed computing used to benefit society. Distributed computing is a powerful way to approach problems that have vast amounts of data that must be processed. These projects allow the user to decide if he wants to participate in the botnet by making the bot software available for download. Once the user downloads and installs the software, the bot contacts the master server and retrieves instructions. The bot computes what is requested of it and relays the information back to the server.

DDoS attacks can be carried out in much the same way. The attackers do not ask the computer owners for permission before using their computers, however. A denial of service attack is a method of attacking a computer system that uses up system resources in an attempt to crash computers, flood the network, or otherwise halt operations at a target site. A DDoS is the same as a DoS attack except that the attack is distributed to several or even thousands of machines which can all work at the same time. Distributing the workload to many computers allows the attacker to be much more efficient and dangerous.

Some bots can be used to help send spam. There are bots running dedicated to system scans. These scans can help locate open proxy servers. Open proxy servers are used by spammers to hide their tracks while sending spam. By forwarding mail through an open proxy, the recipient sees the proxy's address as the sender. Open proxies can also be used for other applications. "Additionally, many computer intruders break into systems specifically to install programs (a.k.a. bots) that enable them to connect to IRC networks without disclosing their actual location. This allows individuals to trade copyright protected media and other illegal

materials through the compromised system rather than directly from their personal computer." (Casey, 2002)

Bots can also be used for general information gathering whether it is on an IRC network or the open Internet. These bots may continuously scan for computers with vulnerabilities, capture packets on the network segment, or search for remote systems with open ports. Some bots are targeted at collecting personal identifiable information such as credit card numbers, passwords, or addresses.

Why create botnets?

As mentioned earlier, some botnets can be beneficial to society. One of the main reasons to create bots is for malicious purposes. Hackers create these bot networks for their personal gain. They can steal personally identifiable information to use against you for identity theft. They may also be looking for usernames and passwords or simply email addresses for which to send spam.

Botnets are a prized commodity on the internet. Hackers are often willing to rent their hard-earned bots for money. An intelligence officer at Scotland's National Hi-Tech Crime Unit provides insight on this activity:

> It may not take much for a bot herder to rent out his botnet, with cold hard cash a pretty big incentive for those involved in virus writing or deploying Trojans. Organised [*sic*] crime groups across Europe and the wider world are making use of these virtual weapons of mass destruction and are targeting lucrative online businesses for DDoS attacks. These attacks are followed by a demand for money in return for the cessation of the attack. Such businesses face the prospect of losing their revenue stream for hours, which they must weigh up against paying any such ransom. Those who pay are inevitably attacked again

> in the future. Such crime groups are actively recruiting IT specialists at an early age and providing them with luxurious lifestyles in return for them turning their skills to criminal purposes. (Barnett, 2005)

The Internet black market continues to grow. Information theft promotes buyers and sellers in this market. Governing the Internet is still in question. There are many issues that have yet to be addressed in terms of jurisdiction and international affairs.

The underground market for botnets is real. Hiring zombie armies is appealing because it takes time and effort to compromise these machines. "Botnets have become so common that they are commodities on the underground market. Botnets of nearly any size are reportedly available for $.06 per machine." (Coursen, 2005)

Botnets obviously vary in size depending on several issues. Computers must be compromised before a hacker can actually use the computer as a zombie. Even after a bot has been installed on a computer, the computer's availability may change if it is powered down or moved behind increased network security. "Honeynet research … noted that the average botnet includes about 2,000 broadband-connected computers; the Multi-State Information Sharing Analysis Center (MS-ISAC), a centrally coordinated mechanism for sharing information security intelligence between states, has reported one containing 350,000 computers." (Cherkin, 2005) The sky is the limit when it comes to botnets. Having more zombies in the botnet gives an attacker more power and flexibility in his attacks. At the same time, it increases his online presence. Many hackers probably use as few bots as possible to conduct attacks. It is easier to find a bundle of needles in a haystack than it is a single needle.

IRC Bots

Many malicious IRC bots exist. One of the most well known is that of the SubSeven Trojan. This bot propagates via IRC DCC Sends. The filename of the file being sent is usually something promising sexually explicit material. Once the file is installed, however, the Trojan has supreme access to the host machine. "Once installed, SubSeven's friendly user-interface allows the attacker to easily monitor a victim's keystrokes, watch a computer's web cam, take screen shots, eavesdrop through the computer's microphone, control the mouse pointer, read and write files, and sniff traffic off the victim's local network." (Poulsen, 2001) Script kiddies could very easily use this software due to its graphical user interface (GUI).

Another well known IRC bot was originally thought to be a worm. Attack Bot was created to exploit a Microsoft Windows server vulnerability. The bot took advantage of the Windows distributed document object model (DCOM) and remote procedure call (RPC) services. Using a buffer overflow technique, the attackers could gain full access to the machine. (Lemos, 2003) Since the software did not propagate autonomously, it was deemed a bot instead of a worm.

In the future expect to see more bots using encryption to hide themselves. One of the methods used to detect bots is that they usually use ports identified with well known programs such as IRC. (Evers, 2005) With the strong push in open source programs, encryption techniques should not be hard to implement into these bots. That is, if these hackers cannot simply find a way to use an existing method of encryption already installed on the client machines.

It is worth noting that there are bots that do not necessarily use IRC to propagate. Trinoo, Tribe Flood Network (TFN), Stacheldraht, and mstream are other infiltration tools that have

taken advantage of buffer overflows to take control of a computer system. (Dittrich et al., 2000) This type of attack can be seen in modern day worms. (Lemos, 2005)

IRC Security

Users should always use secure passwords when using any services on a computer, especially when that system is connected to the Internet. Always run an antivirus program and keep the signatures updated. Even if the system encounters a malicious file, hopefully the antivirus will detect it and isolate the file. Trojan and bot scanners can also be implemented as an extra measure of security. Due to the complex nature of an operating system, it is also imperative that users keep their operating systems patched. When buffer overflows are discovered, the manufacturer will usually release a fix for the code with haste. Invest in a firewall and continue to maintain it. Advanced users should disable any services not necessary for normal operation. These services should only be running when needed and can easily be loaded in the future. Finally, stay educated on current trends, exploits, and intrusion techniques. (EFNET, 2003)

There are features included in many IRC clients that may possibly be a security risk. One of these features is the direct connect client (DCC). DCC sessions do exactly what the name implies—they create a direct connection from user to user without relaying through the server. Never directly connect to a user you do not trust. At the same time, important information should only be sent via DCC Chat when using IRC. DCC Chats are still vulnerable to eavesdroppers and hackers. It is still possible to initiate man-in-the-middle attacks against a DCC Chat. Also, the contents are not encrypted. Plain-text messages are easy to intercept and observe.

Many clients support a feature called Fserve. Fserve is a file server. It allows you to send and receive files from other users. The clients usually come with a way to disable this fileserver, which should remain disabled unless there is a need to use the feature. There is usually also an option available to ignore users. Never trust any users on IRC unless you really know who they are. IRC is one method of virus, Trojan, and other malware propagation.

There are also certain ways in which one should conduct himself when using IRC to help remain safe from attackers. Anonymity is an advantage that a hacker on IRC possesses. This too can be an advantage for the common user. The hacker may try to learn about you in an attempt to conduct a social engineering attack and get by your defenses. IRC is a great tool used to aid in the exchange of ideas online, but there is never a need to distribute personal information via this mode of communication. If information is important to you, it is probably also valuable to a hacker.

Some IRC networks give some extra protective measures. One such network is Gamesurge.net which allows a user to hide his real hostname. Usually, broadband connections use a hostname scheme that includes the cable modem's IP address as part of the string. A user's real hostname may be "nc-AAA-BBB-CCC-DDD.dyn.sprint-hsd.net" where A, B, C, and D are each octet of the IP address. A user mode of "+x" can be set which changes your hostname to that of gamesurge.net. It may then be something like "myusername.gamesurge.net." This obviously has some advantages, but at the same time keep in mind that hackers can also use this feature.

Conclusion

Zombies and botnets are real risks facing the Internet society today. Botnets can cause extreme damage to companies by means of DDoS, information theft, and spam. All computers

connected to the Internet are potential targets for hackers. Organizations and individuals alike must educate themselves about these risks. Zombie armies are forming at this very moment. Always be cautious when using services on the internet. IRC is a good tool to exchange ideas with other users, but be weary of the threats that accompany this service.

Hackers will continue to develop techniques to infiltrate computer systems. Bots, worms, viruses, Trojans, backdoors, and social engineering attacks are not a thing of the past and will surely continue to plague the Internet. When it comes to IRC and botnets, educating the users is probably the best way to minimize risk.

References

Barnett, S. (2005). The IT crimewave. *The Journal*, *50*(7).

Casey, E. (2002). Error, Uncertainty, and Loss in Digital Evidence. *International Journal of Digital Evidence*, *1*(2), 1-45.

Cherkin, S. (2005). The Botnet Threat. Retrieved Nov. 26, 2005, from http://www.ciostrategycenter.com/wcbs/Threat/viruses/the_botnet_threat/.

Coursen, S. (2005). Security Threats: The Landscape Has Changed . *Secure Convergence Journal*.

Dittrich, D., Weaver, G., Dietrich, S., Long, N. (2000). The "mstream" distributed denial of service attack tool. Retrieved Nov. 26, 2005, from http://staff.washington.edu/dittrich/misc/mstream.analysis.txt.

EFNET, (2003). irc.efnet.nl Security Information and Warnings. Retrieved Nov. 26, 2005, from http://www.efnet.nl/security.php.

Evers, J. (2005). Bots may get cloak of encryption. Retrieved Nov. 26, 2005, from News.com Web site: http://news.com.com/Bots+may+get+cloak+of+encryption/2100-7349_3-5952102.html.

Lemos, R. (2003). Attack bot exploits Windows flaw. Retrieved Nov. 26, 2005, from News.com Web site: http://news.com.com/2100-1009-5059263.html.

Lemos, R. (2005). Feds Bust Suspected Bot Master . Retrieved Nov. 26, 2005, from http://enterprisesecurity.symantec.com/content.cfm?articleid=6156.

Merriam-Webster Online Dictionary, (2005). Zombie. Retrieved Nov. 19, 2005, from http://www.m-w.com/dictionary/zombie.

Oikarinen, J. (n.d.). IRC History. Retrieved Nov. 19, 2005, from http://www.irc.org/history_docs/jarkko.html.

Oikarinen, J., & Reed, D. (1993). Internet relay chat protocol. Retrieved Nov. 19, 2005, from Request for Comments: 1459 Web site: ftp://ftp.irc.org/irc/docs/rfc1459.txt.

Poulsen, K. (2001). New subseven trojan unleashed. Retrieved Nov. 26, 2005, from http://www.theregister.co.uk/2001/03/13/new_subseven_trojan_unleashed/.

Schluting, C. (2005). Botnets: Who Really "0wns" Your Computers?. Retrieved Nov. 26, 2005, from http://www.enterprisenetworkingplanet.com/netsecur/article.php/3504801.

Webopedia, (2002). Zombie. Retrieved Nov. 19, 2005, from http://www.webopedia.com/TERM/z/zombie.html.

Wikipedia, (2005). Botnet. Retrieved Nov. 25, 2005, from http://en.wikipedia.org/wiki/Botnet.